



R E P U B L I Q U E F R A N C A I S E



#  
5

WS



J1036 U.S. PTO

09/900337



07/06/01

# BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

## COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 01 MARS 2001

Pour le Directeur général de l'Institut  
national de la propriété industrielle  
Le Chef du Département des brevets

Martine PLANCHE

**CERTIFIED COPY OF  
PRIORITY DOCUMENT**

INSTITUT

SIEGE  
26 bis, rue de Saint Petersburg  
75800 PARIS cedex 08

**THIS PAGE BLANK (USPTO)**



26 bis, rue de Saint Pétersbourg  
75800 Paris Cedex 08  
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

# BREVET D'INVENTION CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI



REQUÊTE EN DÉLIVRANCE 1/2

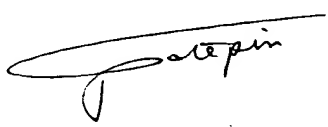
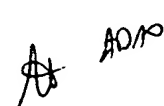
Cet imprimé est à remplir lisiblement à l'encre noire

08 540 W / 260899

<b>REMISE DES PIÈCES</b> DATE <b>11 JUIL 2000</b> LIEU <b>75 INPI PARIS</b>  N° D'ENREGISTREMENT <b>0009049</b> NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI <b>11 JUIL. 2000</b>		<b>1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE</b>  Monsieur Philippe GATEPIN Société Civile S.P.I.D. 156 Bd Haussmann 75008 PARIS	
<b>Vos références pour ce dossier</b> (facultatif) PHFR000073			
<b>Confirmation d'un dépôt par télécopie</b> <input type="checkbox"/> N° attribué par l'INPI à la télécopie			
<b>2 NATURE DE LA DEMANDE</b>		<b>Cochez l'une des 4 cases suivantes</b>	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
Demande de brevet initiale		N°	Date
ou demande de certificat d'utilité initiale		N°	Date
Transformation d'une demande de brevet européen		<input type="checkbox"/>	Date
Demande de brevet initiale		N°	Date
<b>3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)</b> Système de communication, émetteur, méthode de protection contre des erreurs de transmission.			
<b>4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE</b>		Pays ou organisation Date N° Pays ou organisation Date N° Pays ou organisation Date N° <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
<b>5 DEMANDEUR</b>		<input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»	
Nom ou dénomination sociale		KONINKLIJKE PHILIPS ELECTRONICS N.V.	
Prénoms			
Forme juridique		Société de droit Neerlandais	
N° SIREN			
Code APE-NAF			
Adresse	Rue	Groenewoudseweg 1	
	Code postal et ville	5621 BA EINDHOVEN	
Pays		PAYS-BAS	
Nationalité		Néerlandaise	
N° de téléphone (facultatif)			
N° de télécopie (facultatif)			
Adresse électronique (facultatif)			

**BREVET D'INVENTION  
CERTIFICAT D'UTILITÉ**

REQUÊTE EN DÉLIVRANCE 2/2

REMISE DES TIÈGES DATE <b>11 JUIL 2008</b> LIEU <b>75 INPI PARIS</b> N° D'ENREGISTREMENT <b>0009049</b> NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI	
<b>Vos références pour ce dossier :</b> <i>(facultatif)</i>		PHFR000073	
<b>6 MANDATAIRE</b>			
Nom		GATEPIN	
Prénom		Philippe	
Cabinet ou Société		S.P.I.D.	
N° de pouvoir permanent et/ou de lien contractuel		07036 - Délégation de pouvoir 8819	
Adresse	Rue	156 Bd Haussmann	
	Code postal et ville	75008	PARIS
N° de téléphone <i>(facultatif)</i>		01 40 76 80 30	
N° de télécopie <i>(facultatif)</i>			
Adresse électronique <i>(facultatif)</i>			
<b>7 INVENTEUR (S)</b>			
Les inventeurs sont les demandeurs		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non Dans ce cas fournir une désignation d'inventeur(s) séparée	
<b>8 RAPPORT DE RECHERCHE</b>		Uniquement pour une demande de brevet (y compris division et transformation)	
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> <input type="checkbox"/>	
Paiement échelonné de la redevance		Paiement en trois versements, uniquement pour les personnes physiques <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non	
<b>9 RÉDUCTION DU TAUX DES REDEVANCES</b>		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention <i>(joindre un avis de non-imposition)</i> <input type="checkbox"/> Requête antérieurement à ce dépôt <i>(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence)</i>	
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes			
<b>10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE</b> (Nom et qualité du signataire) P. GATEPIN Mandataire SPID 422-5/S008		<b>VISA DE LA PRÉFECTURE OU DE L'INPI</b>  	

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg

75800 Paris Cedex 08

Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

DÉSIGNATION D'INVENTEUR(S) Page N° 1. / 1.

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 260299

<b>Vos références pour ce dossier</b> (facultatif)		PHFR000073	
<b>N° D'ENREGISTREMENT NATIONAL</b>		000 9049	
<b>TITRE DE L'INVENTION</b> (200 caractères ou espaces maximum) Système de communication, émetteur, méthode de protection contre des erreurs de transmission.			
<b>LE(S) DEMANDEUR(S) :</b> KONINKLIJKE PHILIPS ELECTRONICS N.V.			
<b>DESIGNE(NT) EN TANT QU'INVENTEUR(S) :</b> (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
<b>Nom</b>		BONIFAS	
<b>Prénoms</b>		Jean-Luc	
<b>Adresse</b>	<b>Rue</b>	156, Bd Haussmann	
	<b>Code postal et ville</b>	75008	PARIS
<b>Société d'appartenance</b> (facultatif)			
<b>Nom</b>			
<b>Prénoms</b>			
<b>Adresse</b>	<b>Rue</b>		
	<b>Code postal et ville</b>		
<b>Société d'appartenance</b> (facultatif)			
<b>Nom</b>			
<b>Prénoms</b>			
<b>Adresse</b>	<b>Rue</b>		
	<b>Code postal et ville</b>		
<b>Société d'appartenance</b> (facultatif)			
<b>DATE ET SIGNATURE(S)</b> <b>DU (DES) DEMANDEUR(S)</b> <b>OU DU MANDATAIRE</b> (Nom et qualité du signataire) 11 Juillet 2000 P.GATEPIN Mandataire SPID 422-5/S008			

**THIS PAGE BLANK (USPTO)**

## **DESCRIPTION**

L'invention concerne une méthode de protection contre des erreurs de transmission, de trames de données primaires numériques comprenant des données primaires de priorités différentes, pour délivrer sur un canal de communication des trames de données protégées contre les erreurs de transmission.

Elle concerne également un système de communication incluant un émetteur pour transmettre des trames de données primaires numériques à un récepteur via un canal de communication, cet émetteur étant pourvu de moyens adaptés pour mettre en œuvre la méthode précédemment mentionnée.

Elle a de nombreuses applications dans les systèmes de communication de données multimédias en général, comme c'est notamment le cas dans les applications de type vidéophonie sur réseaux mobiles ou filaires.

Le brevet européen publié sous le numéro 0 680 157 A1 décrit une méthode et un système pour contrôler la protection aux erreurs des données transmises à partir d'un émetteur à un récepteur, sur une voie de transmission. Cette méthode met en œuvre une protection des données à transmettre en utilisant au mieux la bande passante disponible sur la voie de transmission. Pour cela, les données à transmettre sont dans un premier temps classées suivant différents niveaux d'importance, et sont dans un second temps encodées selon un algorithme ayant pour but de leur ajouter des données de redondance. Cet ajout de données de redondance tient compte du niveau d'importance des données à transmettre afin de faire varier la puissance de protection.

La méthode de protection contre les erreurs de transmission mise en œuvre dans le document de l'art antérieur présente un certain nombre d'inconvénients.

Tout d'abord, la puissance de protection est définie à l'avance, si bien que cette méthode ne prend pas en compte d'éventuels changements relatifs à la qualité de transmission pouvant remettre en question la puissance de protection des données à transmettre. Cette méthode souffre donc d'un manque d'adaptation de la protection des données à des conditions fluctuantes de transmission, ce qui se traduit dans ces conditions d'une part par une mauvaise occupation de la bande passante de la voie de transmission, mais aussi par une mauvaise protection des données transmises.

D'autre part, la méthode décrite implique la mise en œuvre d'une architecture rigide nécessitant de définir à l'avance le nombre de niveaux d'importance des données à protéger. Cette rigidité de l'architecture se traduit par la mise en œuvre d'une chaîne de traitement des données, pour chacun des niveaux d'importance. Il y a donc autant de chaîne de traitement qu'il y a de niveaux d'importance, ce qui conduit à une solution coûteuse et peu flexible.

L'invention a pour but de remédier dans une large mesure à ces inconvénients en proposant un système de communication, un émetteur, ainsi qu'une méthode, ayant pour but de protéger de façon sélective des trames de données primaires transmises sur un canal de communication, d'une façon plus fiable et moins coûteuse que celle décrite dans le document de l'art antérieur.

A cet effet, la présente invention est caractérisée en ce que la méthode de protection comprend :

- 10 a) une étape d'attribution d'un niveau de priorité à chacune des trames de données primaires,
- b) une étape d'aiguillage pour sélectionner, en fonction de leur niveau de priorité, les trames de données primaires nécessitant une protection contre des erreurs de transmission,
- 15 c) une étape de protection contre les erreurs de transmission pour ajouter des données de redondance aux trames de données primaires sélectionnées, en fonction du niveau de priorité de la trame primaire considérée et de la qualité du canal de communication, afin de délivrer lesdites trames de données protégées.

20 La méthode de protection selon l'invention comporte un ensemble générique d'étapes de traitement conduisant à délivrer des données protégées contre des erreurs de transmission sur un canal de communication. Cet ensemble d'étapes de traitement est appliqué à toutes les données primaires faisant l'objet d'une protection contre les erreurs. Dans un premier temps, les données primaires étant supposées être de plusieurs types, une détection de leur type est effectuée. A l'aide d'une table de correspondance, une priorité relative aux données primaires est alors déterminée pour d'une part en informer l'étape de protection effectuant la protection contre les erreurs, et pour d'autre part prendre une décision portant sur la possibilité ou la nécessité de protéger lesdites données primaires. En effet, l'étape de protection contre les erreurs de transmission consistant à ajouter des informations de redondance aux données primaires, il est ainsi possible de ne pas protéger les données d'un certain type s'il est jugé que cela conduirait à une augmentation trop importante des données transmises sur le canal de communication, ou s'il est jugé que la priorité des données est suffisamment basse pour s'affranchir d'une protection contre les erreurs. L'étape de protection aux erreurs, du type FEC (de l'anglais Forward Error Correction), permet de délivrer lesdites données protégées à partir desdites données primaires, de leur priorité associée et d'une valeur renseignant sur la qualité du canal de communication. Cette étape de protection de type FEC, par exemple selon la norme IETF RFC 2733 dans le contexte de transmission de paquets RTP (de l'anglais Real Time Protocol), permet d'ajouter à chaque type de données primaires une quantité d'informations de redondance tenant compte à la fois de leur priorité et de ladite valeur renseignant sur la qualité

du canal de communication. En effet, la quantité d'informations de redondance est d'autant plus grande que la priorité des données primaires est élevée et que la qualité du canal de communication est mauvaise. La méthode décrite est ainsi générique puisqu'une seule chaîne de traitement est mise en œuvre quel que soit le type de données primaires à traiter, peu coûteuse puisque l'on ne multiplie pas les chaînes de traitement en fonction des différents types de données primaires, et flexible puisque le nombre de données de redondance ajoutées aux données primaires est adapté à la qualité courante du canal de communication.

L'invention concerne également un émetteur inclus dans un système de communication de type radiotéléphonie par exemple, dont le fonctionnement pourra bénéficier des possibilités de protection contre les erreurs décrites ci-dessus. L'invention prévoit en effet un ensemble générique de traitement desdites données primaires pour transmettre à un récepteur des données protégées contre des erreurs de transmission. L'émetteur règle ainsi le niveau de redondance des données envoyées de façon adaptée au niveau de priorité des données et à la qualité du canal de transmission, tout en garantissant un compromis optimal entre l'occupation de la bande passante du canal de transmission et le niveau de protection contre les erreurs.

Ces aspects de l'invention ainsi que d'autres aspects plus détaillés apparaîtront plus clairement grâce à la description suivante, faite en regard des dessins ci-annexés, le tout donné à titre d'exemple non limitatif, dans lesquels :

La figure 1 est un schéma fonctionnel décrivant l'enchaînement des différentes opérations selon l'invention,

La figure 2 est un schéma décrivant un système de communication comprenant un émetteur selon l'invention.

La figure 1 décrit schématiquement les différentes étapes conduisant à la protection des données primaires envoyées par un émetteur sur un canal de communication.

L'ensemble 101 des différentes étapes permet de délivrer, à partir de données primaires 109, des données 107 protégées contre les erreurs de transmission et/ou des données 108 n'ayant subi aucun traitement de protection contre les erreurs. Les données primaires 109 correspondent à des trames de données numériques issues d'un encodeur audio/vidéo par exemple, ou de façon plus générale issues d'une source de données numériques de données multimédias. Ces trames de données primaires sont par exemple issues d'un encodeur audio/vidéo de la famille MPEG-1/MPEG-2 ou de la famille H.323/H.324. Ce type de données présente la caractéristique de comprendre des types différents de données permettant de les identifier et de les synchroniser lors de leur décodage. Dans le contexte de l'invention, ces différents types de données sont interprétés et traduits en niveaux de priorité. En effet, il existe

une certaine hiérarchie de telles données qui permet de décrire le contenu informationnel délivré par ladite source. Par exemple, si les données primaires 109 sont relatives à des données vidéo encodées selon la norme MPEG-2, les données relatives aux images, slices et macro-blocks définissent une structure hiérarchique imbriquée de priorité décroissante dans laquelle il est préférable de protéger contre les erreurs les données relatives aux images, c'est-à-dire aux données ayant le type le plus prioritaire. Pour cela, il est prévu une étape 102 de détection du type des données ou trames de données primaires 109 afin de leur associer un niveau de priorité. Cette détection se base sur l'analyse de la syntaxe d'encodage des données primaires 109, en repérant notamment des mots-clés de la syntaxe contenus dans les différents entêtes (Headers en anglais). Dans une autre variante de l'invention, il pourra être envisagé de ne pas faire de détection du type des données 109, cette information de type étant directement fournie par des éléments extérieurs, tels que l'encodeur ou la source délivrant les données 109. Cette variante est référencée en 110. Une fois que le type des données primaires est connu, une correspondance est établie à l'étape 103 entre ladite information de type et un niveau de priorité. Cette étape, davantage détaillée par la suite, consiste en la mise en œuvre d'une table de correspondance dans laquelle un utilisateur a préalablement établi une correspondance entre chaque type de données et un niveau de priorité. Le nombre de correspondances n'étant limité par aucune contrainte, cette méthode peut dès ce niveau de traitement être adaptée à différentes sources de données contenant des types de données en nombre différent. Il suffit pour cela de prévoir une table de correspondance comportant un nombre de correspondances suffisamment grand, quitte à ne pas toutes les utiliser si les données primaires comportent un faible nombre de types. L'étape 103 délivre ainsi une valeur relative à la priorité des données ou trames de données primaires 109. Suivant la valeur de ce niveau de priorité, les données 109 sont effectivement protégées contre les erreurs de transmission, ou alors ne subissent aucun traitement supplémentaire. L'élément 106 est chargé de ce choix permettant l'orientation des données primaires 109 dans la chaîne de traitement 101. Il peut en effet être décidé de ne pas protéger les données primaires dont la priorité est faible, cela signifiant que l'on est soit en présence de données de faible importance ne justifiant pas une protection, soit de données pouvant être reconstruites après transmission même après avoir subi de nombreuses erreurs. Dans ces cas, les données 109 ne sont pas protégées contre les erreurs afin de ne pas surcharger inutilement la bande passante du canal de communication sur lequel sont envoyées les données primaires. Dans le cas contraire où la priorité des données primaires est jugée suffisamment élevée, l'élément 106 aiguille les données 109 vers l'étape 104 de protection contre les erreurs. Cette étape de protection a pour but d'ajouter des données de redondance aux données primaires 109 pour pouvoir reconstruire ces mêmes données primaires après transmission, même si celles-ci subissent de nombreuses erreurs lors de leur transmission. L'étape 104 permet de délivrer des données 107 protégées contre les erreurs de transmission en mettant en œuvre de façon spécifique et innovante un algorithme de type FEC. L'invention prévoit à cet effet une protection sélective des données primaires dans le sens où la quantité de

redondance, exprimée par exemple en pourcentage du volume en octets des données primaires auxquelles s'applique cet ajout de redondance, tient compte de la priorité des données primaires. En d'autres termes, le pourcentage de redondance ajoutée aux données primaires sera d'autant plus grand que le niveau de priorité sera élevé. Cet aspect de l'invention sera  
5 davantage détaillé par la suite. De cette façon, il est à la fois possible de garantir une protection optimale des données importantes, tout en ne transmettant pas sur le canal de communication des données de redondance ajoutées à des données primaires de faible niveau de priorité, le canal de communication n'étant pas alors inutilement encombré. L'étape de protection 104 reçoit, en plus des données 109 et de la valeur renseignant sur leur niveau de priorité, une  
10 valeur 105 reflétant la qualité Q du canal de transmission. Cette valeur reflète par exemple le taux d'erreurs du canal de communication estimé par le nombre de trames de données perdues sur ce canal pendant une certaine durée, cette estimation étant faite au niveau d'un dispositif distant et le résultat de cette étape d'estimation envoyé à l'émetteur. De cette façon, la quantité de redondance ajoutée aux données primaires est modulée par cette valeur de qualité  
15 du canal de communication : la quantité de redondance ajoutée aux données primaires est d'autant plus élevée que cette valeur de qualité reflète un taux d'erreurs important. Les données primaires ne sont ainsi pas protégées suivant une valeur arbitraire de la qualité du canal de communication, mais suivant une valeur de qualité reflétant les caractéristiques réelles dudit canal : le degré de protection est parfaitement adapté aux conditions de transmission des  
20 données.

La protection contre les erreurs de transmission est ainsi assurée par une double stratégie menée conjointement pour permettre de quantifier les données de redondance à  
ajouter aux données primaires, cette stratégie comprenant :

- 25 - une évaluation d'une première quantité de données de redondance faite suivant le niveau de priorité des données primaires, cette première quantité étant d'autant plus importante que le niveau de priorité est élevé,
- une modulation de cette première quantité de données de redondance faite suivant une  
30 valeur reflétant la fiabilité et la qualité du canal de communication, cette modulation se traduisant par une augmentation d'autant plus grande des données de redondance que le canal de communication est peu fiable ou que le taux d'erreurs de transmission est élevé, cette augmentation des données de redondance étant bien sûr limitée par la bande  
passante maximale du canal de transmission.

35 La figure 2 décrit un système de communication comprenant un émetteur selon l'invention. Ce système de communication comprend un émetteur E communiquant via un canal de communication 217 de type filaire ou hertzien, avec un récepteur R recevant les données protégées en vue de les utiliser dans des applications de type multimédia par exemple. Ce système de communication correspond par exemple à une application utilisant la norme H.323

(utilisant le protocole de transmission RTP) relative à la transmission de vidéo sur Internet, ou à la norme H.324 (utilisant le protocole de transmission de la norme H.223) relative à une application de type vidéotéléphonie, ou à une application de type GSM, ou à une application mettant en œuvre la norme Bluetooth.

5

L'émetteur E comprend une source 218 de données ou de trames de données primaires numériques 209 issues par exemple d'un serveur ou d'un encodeur audio/vidéo, et envoyées au module de protection contre les erreurs 201. Parallèlement à ces données primaires, le module 201 reçoit un signal 205 renseignant sur la qualité du canal de transmission 217. A cet effet, il est possible d'exploiter le protocole RTCP (de l'anglais Real Time Control Protocol), défini conjointement avec le protocole RTP selon la norme RFC 1889 IETF, pour utiliser les statistiques qu'il permet de délivrer portant sur la qualité de la communication, telles que le nombre de paquets de données perdus depuis le dernier paquet RTCP reçu au niveau du récepteur R. Cette estimation de la qualité du canal de communication est effectuée par le bloc 225 qui transmet à l'émetteur le résultat de son estimation via le signal 205. Bien sûr, tout autre moyen, un moyen propriétaire par exemple, pourra être mis en œuvre pour délivrer une information 205 reflétant la qualité du canal de transmission. Le module 201, selon la description faite en regard de la figure 1, délivre à partir des données primaires 209, soit des données sans protection 208, soit des données 207 protégées par l'ajout de données de redondance, le degré de protection des données primaires dépendant à la fois de leur niveau de priorité et de la qualité de transmission 217. Par la suite, la description sera faite de façon non restrictive sur la base d'une application selon le protocole RTP.

Dans un mode de réalisation préféré, considérons un système de communication pouvant effectuer l'envoi de données encodées selon la norme MPEG-4 entre un émetteur selon l'invention et un récepteur, via un canal de communication utilisant la norme Bluetooth. Dans ce cas, et selon le choix de l'utilisateur, les données vidéo de type GOV (de l'anglais Group of Video Object Plane), les données d'estimation de mouvement MV (de l'anglais Motion Vector), et les données de TEXTURE constituent trois types de données de priorité  $p(\ )$  décroissante :  $p(\text{GOV}) > p(\text{MV}) > p(\text{TEXTURE})$ . En effet, il peut être donné un haut niveau de priorité au type GOV, un niveau moyen de priorité au type MV, et un niveau bas de priorité au type TEXTURE en considérant que les données correspondantes à ce dernier type ne sont pas indispensables à l'application et que des erreurs ou des pertes de ces données ne sont que faiblement dommageables. Ainsi, trois degrés de protection des données primaires sont définis par le module 201 pour une certaine qualité Q1 du canal de communication :

35

- a) ajout de 100 % de données de redondance aux données de type GOV,
- b) ajout de 50 % de données de redondance aux données de type MV,
- c) ajout de 5 % de données de redondance aux données de type TEXTURE.

Avec une qualité  $Q_2$  de transmission sur le canal de communication, plus mauvaise que dans le scénario précédent, c'est-à-dire avec  $Q_2 < Q_1$ , les trois degrés de protection des données primaires sont maintenant définis par :

- a) ajout de 200 % de données de redondance aux données de type GOV,
- 5        b) ajout de 60 % de données de redondance aux données de type MV,
- c) aucun ajout de données de redondance aux données de type TEXTURE.

Cet exemple illustre parfaitement la double stratégie décrite précédemment pour permettre de quantifier les données de redondance à ajouter aux données primaires, dans le sens où le volume de données de redondance dépend non seulement de la priorité des données mais aussi de la qualité du canal de communication : ici, dans le cas où  $Q=Q_2$ , et comparativement au cas où  $Q=Q_1$ , les données de redondance sont principalement renforcées sur les données de type GOV, contrairement aux données de type MV dont la quantité de redondance n'augmente que faiblement, d'une part parce qu'elles n'ont pas un niveau de priorité élevé, et d'autre part pour ne pas saturer le canal de communication. Quant aux données de type TEXTURE, aucune donnée de redondance n'est ajoutée dans le cas où  $Q=Q_2$  puisque leur niveau de priorité est le plus faible et que tout l'effort de protection est mis sur les données de type GOV.

Ces données analysées et/ou traitées par 201 sont alors envoyées vers le module 220 ayant pour fonction de les formater selon le protocole RTP, notamment en ajoutant à chacune des trames de données un entête RTP spécifique à la protection FEC afin de synchroniser les données primaires et les données de redondance correspondantes au niveau du récepteur. Le module 220 envoie ainsi des trames de données 210 et 211 formatées selon le protocole RTP, à partir des données 207 et 208 respectivement. Chacune des trames de données 210 et 211 est envoyée sur le canal de communication 217 via la couche de transport 221.

Au niveau du récepteur R, les trames de données reçues via la couche de transport 224 sont divisées en deux classes : les trames de données 213 n'ayant subi aucune protection contre les erreurs, et les trames de données 212 ayant fait l'objet d'une protection de type FEC contre les erreurs. Envoyées au module 223, les trames de données 212 et 213 sont analysées en vue de supprimer leur syntaxe associée relative au protocole RTP, ladite syntaxe servant à synchroniser les différentes trames de données reçues. Le module 223 délivre ainsi au module 222, des trames de données 215 exemptes de protection, et des trames de données 214 contenant à la fois des données primaires et des données de redondance. A ce niveau, les trames 215 et 214 correspondent aux trames 208 et 207 respectivement, sauf si des erreurs sont survenues lors de la transmission sur le canal 217, d'où le module 222 ayant pour objet de reconstruire les données entachées d'erreurs :

- soit à partir des seules données 215 non protégées de contenu ayant un faible niveau de priorité, principalement à partir d'interpolation sur des données précédemment reçues non corrompues,
- soit en utilisant les données de redondance associées aux trames de données 214, en appliquant un algorithme de type FEC décrit par la norme RFC 2733. Bien sûr, la réussite de cette reconstruction des données primaires envoyées sera d'autant plus probable que le rapport correspondant au nombre d'erreurs présentes sur la quantité de données de redondance sera faible.

10 Les données 216 ainsi reconstruites et exemptes d'erreurs sont alors envoyées à une application 219, par exemple pour être décodées et affichées sur un écran s'il s'agit de données de type vidéo.

15 Les différentes étapes selon l'invention permettant de délivrer des trames de données protégées peuvent être implémentées au niveau de l'émetteur de différentes façons, notamment en utilisant un processeur de signal exécutant un jeu d'instructions relatif aux traitements 102/106/104 opérés sur des trames de données primaires, et en utilisant une mémoire dont le contenu permet d'établir la correspondance type/priorité relative à l'étape 103.

20 Ainsi ont été décrits et illustrés un système de communication, un émetteur, ainsi qu'une méthode permettant de protéger de façon sélective contre les erreurs, des données transmises sur un canal de communication sujet aux erreurs. Bien entendu, de nombreuses variantes pourront être apportées aux modes de réalisation décrits sans sortir du cadre de l'invention.

25

## REVENDEICATIONS

1. Système de communication entre un émetteur et un récepteur, l'émetteur transmettant au récepteur via un canal de communication des trames de données primaires numériques protégées contre des erreurs de transmission,

5 **caractérisé en ce que** l'émetteur comprend :

  - a) des moyens d'attribution d'un niveau de priorité à chacune des trames de données primaires,
  - 10 b) des moyens d'aiguillage pour sélectionner, en fonction de leur niveau de priorité, les trames de données primaires nécessitant une protection contre des erreurs de transmission,
  - 15 c) des moyens de protection contre les erreurs de transmission pour ajouter des données de redondance aux trames de données primaires sélectionnées, en fonction du niveau de priorité de la trame primaire considérée et de la qualité du canal de communication, afin de délivrer lesdites trames de données protégées.
2. Système de communication selon la revendication 1, **caractérisé en ce que** :

  - a) l'émetteur comprend des moyens pour identifier le type de données contenues dans chacune des trames de données primaires,
  - 20 b) le niveau de priorité associé à chacune des trames de données primaires est déterminé à partir d'une table de correspondance stockée en mémoire, cette table effectuant la correspondance entre le type de la trame primaire considérée et un niveau de priorité.
- 25 3. Système de communication selon la revendication 1 **caractérisé en ce que** le récepteur comprend des moyens d'estimation de la qualité du canal de communication, ainsi que des moyens de transmission via le canal de communication du résultat de cette estimation à l'émetteur.
- 30 4. Emetteur pour délivrer sur un canal de communication, des trames de données primaires numériques de priorités différentes protégées contre des erreurs de transmission,

**caractérisé en ce que** l'émetteur comprend :

  - a) des moyens d'attribution d'un niveau de priorité à chacune des trames de données primaires,
  - 35 b) des moyens d'aiguillage pour sélectionner, en fonction de leur niveau de priorité, les trames de données primaires nécessitant une protection contre des erreurs de transmission,
  - c) des moyens de protection contre les erreurs de transmission pour ajouter des données de redondance aux trames de données primaires sélectionnées, en fonction

du niveau de priorité de la trame primaire considérée et de la qualité du canal de communication, afin de délivrer lesdites trames de données protégées.

5. Emetteur selon la revendication 4 **caractérisé en ce qu'il** comprend des moyens pour identifier le type de données contenues dans chacune des trames primaires, le niveau de priorité associé à chacune des trames de données primaires étant alors déterminé à partir d'une table de correspondance stockée en mémoire, cette table effectuant la correspondance entre le type ainsi identifié et un niveau de priorité.
6. Méthode de protection contre des erreurs de transmission, de trames de données primaires numériques comprenant des données primaires de priorités différentes, pour délivrer sur un canal de communication des trames de données protégées contre les erreurs de transmission,
- caractérisée en ce que** la méthode comprend :
- a) une étape d'attribution d'un niveau de priorité à chacune des trames de données primaires,
  - b) une étape d'aiguillage pour sélectionner, en fonction de leur niveau de priorité, les trames de données primaires nécessitant une protection contre des erreurs de transmission,
  - c) une étape de protection contre les erreurs de transmission pour ajouter des données de redondance aux trames de données primaires sélectionnées, en fonction du niveau de priorité de la trame primaire considérée et de la qualité du canal de communication, afin de délivrer lesdites trames de données protégées.
7. Méthode selon la revendication 6 **caractérisée en ce qu'elle** comprend une étape d'identification du type de données contenues dans chacune des trames primaires, le niveau de priorité associé à chacune des trames de données primaires étant alors déterminé par une étape de mise en correspondance entre le type ainsi identifié et un niveau de priorité.
8. Equipement téléphonique comportant un émetteur selon la revendication 4.

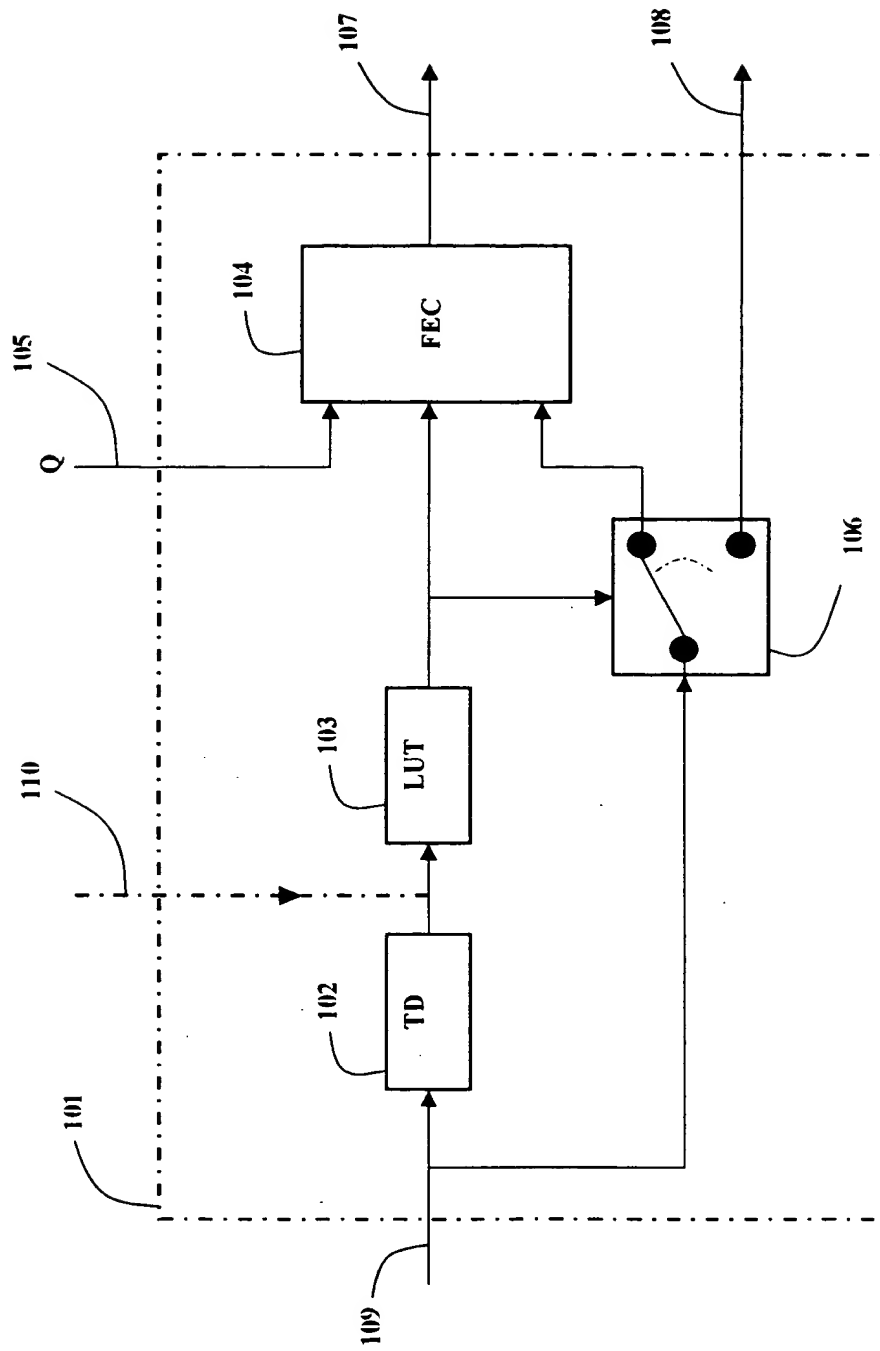


FIG.1

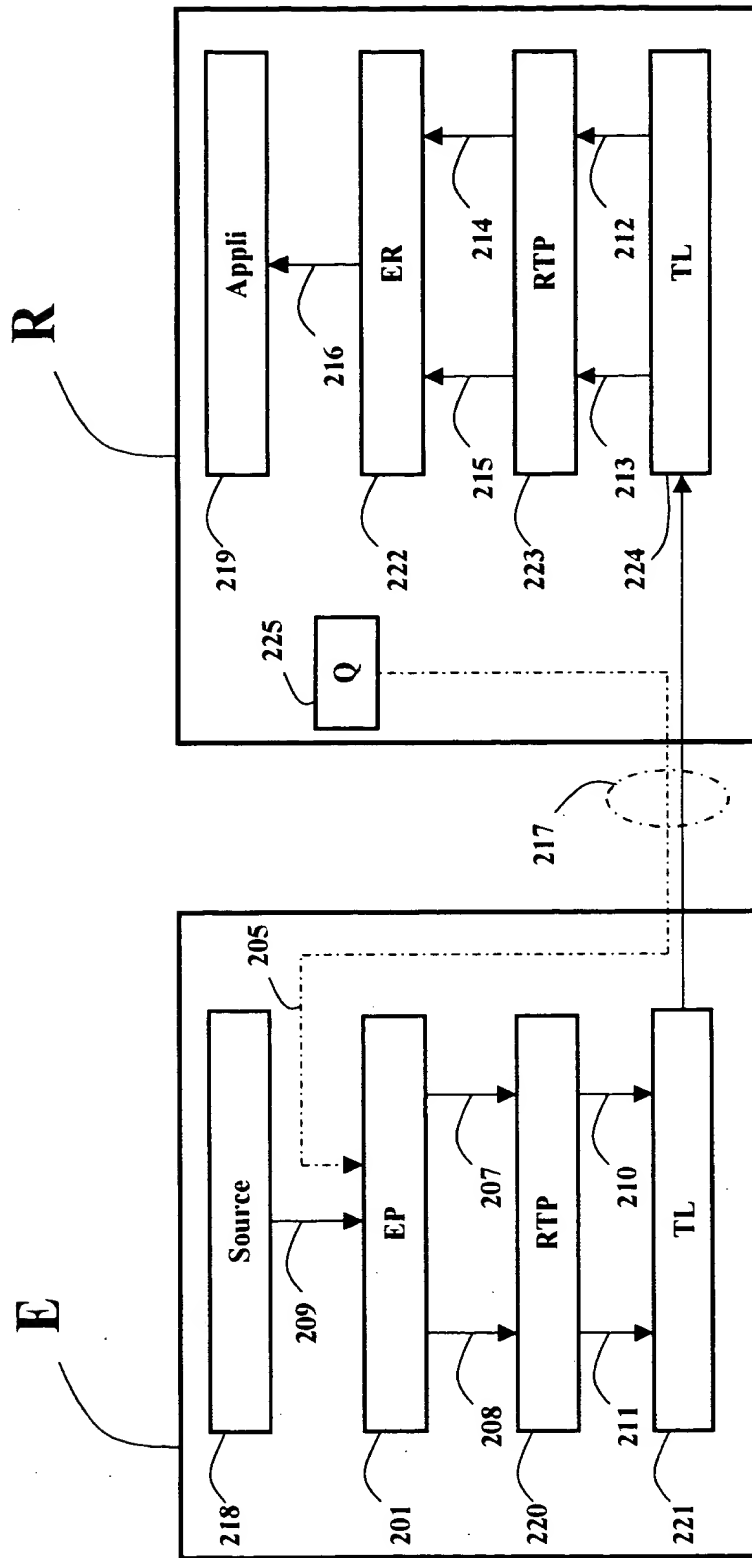


FIG.2